# ITU-T SG17 회의

**나재훈**
TTA 응용보안 및 평가인증 PG 의장,
ITU-T SG17 Q.7 라포처, ETRI 인프라보호연구팀

## 1. 머리말

2011년 4월 11일(월)~20일(수), 스위스 제네바에서 개최된 ITU-T SG17(정보보호) 회의는 ITU 회원국 28개 국가에서 총 143명이 참석했으며, 그 중 한국에서는 15명이 참가했다.

이번 회의에서 한국 주도 하의 개발된 표준초안 3건이(X.1057: Asset management guidelines in telecommunication organizations, X.1192: Functional requirements and mechanisms for the secure transcodable scheme of IPTV, X.1090: Authentication framework with one-time telebiometric template) Consent와, 3건이(X.1211: Usability of network traceback, X.1246: Real-time blocking list(RBL)-based framework for countering VoIP spam, X.1253: Security guidelines for identity management systems) Determine 들어갔다. 그리고 신규로 4건의(X.sisnego[1]: Framework of security information sharing negotiation, X.iptvsec-8: Virtual machine-based security platform for renewable IPTV service and content protection(SCP), X.sap-6: One time password based Non-repudiation framework, X.tif: Integrated framework for telebiometric data protection in e-health and worldwide telemedicines) 표준초안이 작업 아이템으로 채택되었다.

## 2. 주요 회의 내용

ITU-T SG17 표준회의에서는 아프리카 국가들의 대표들이 많이 참석하였으며, 이들을 위한 튜토리얼이 준비되었다는 것이 특징이라 할 수 있겠다. SG17에서는 현재 두 개의 큰 축을 중심으로 표준이 진행되고 있는데, CyberSecurity와 IdM(Identity Management) 이다. CyberSecurity 영역에서는 DDoS의 영향으로 사이버 상에서의 역기능들을 관리하기 위한 관제 시스템 구축을 위한 표준들이 주종을 이루고 있으며, IdM은 아이덴티티 자체에 대한 표준활동 보다는 웹 환경에서

1) TAP: Traditional Approval Process

의 인증 및 인가와 같은 영역으로 확장을 추진하고 있으며, 이는 Q.7의 연구 영역과 상충되고 있다. 그리고 이번 회의의 또 다른 이슈는 차기 회기(2013 ~ 20116년)를 대비한 구조조정에 대한 이야기가 조심스럽게 거론되었다. 주요 내용으로는 업무 양이 과다하게 집중되는 Question의 분할 및 연구아이템이 부족한 Question의 통폐합, 그리고 신규 연구아이템의 배분 등이 주요 이슈가 되고 있다. 이러한 구조조정과 맞물려 클라우드 정보보호 관련하여 열띤 토론을 벌였다.

### 2.1 Cybersecurity

2010년 12월 회의에서는 TAP(Traditional Approval Procedure) 승인 절차에 들어갔던 주요 표준안들이(X.1500: Cybersecurity information exchange techniques, X.1520: Common vulnerabilities and exposures, X.1521: Common vulnerability scoring system) 이번 회의에서 제정(Approval)되었으며, 두 개의 표준이(X.1570(cybex-disc): Discovery mechanisms in the exchange of cybersecurity information, X.tb-ucc: Usability of network traceback) TAP 승인 절차에 들어갔다.

그리고 현재 Q.4에서는 11개의 CYBEX 문서가 개발 중에 있으며, 다음과 같은 주제로 개발 중에 있다.

- Botnets: best practices against botnets and a framework for botnet detection and response
- Abnormal traffic detection and control guideline for telecommunication network
- Malware: guideline on preventing malicious code spreading
- Policy Distribution: Mechanism and procedure for distributing policies for network security
- Attacks: framework for countering cyber attacks in SIP-based services
- Traceback: capabilities and mechanisms
- A possible cybersecurity index
- Preventing web-based attacks

### 2.2 IdM

SG17 내에서의 IdM은 그 영역을 확장하려고 적극적인 활동을 하고 있다. IdM은 인증서, 식별자, 그에 따르는 속성에 대한 생명주기인 생성, 유지, 이용, 폐지에 따르는 관리를 목적으로 한다.

그러나 담당 연구과제인 Q10은 IdM의 ToR을 새로 개발을 하고자 하는 의도를 보이고 있다. 즉 인식자의 생성, 이용, 폐지에 대한 표준개발을 넘어서, 도메인 간의 신뢰정보의 전달 및 판단을 위한 인증 영역의 표준개발을 하고 있으며, 더 나아가 CYBEX와의 연계를 의도하고 있다. SG17의 전반적인 역할분담을 깨트리고 있는 상황이다.

현재 개발 중인 표준문서 X.eaa(Information technology - Security techniques - Entity authentication assurance)는 ISO/IEC와 공동으로 개발하고 있으며, 이 표준은 엔티티의 인증보증을 관리하는 프레임워크를 제공함을 목표로 하고 있다. 그 주요 내용으로는 엔티티 인증보증의 4가지 수준, 4가지 수준에 대한 기준 및 가이드라인, 다른 인증보증 스킴과의 연계를 위한 가이드, 및 위협을 약화시키기 위한 통제를 위한 가이드를 포함한다.

또한 웹 정보보호 표준관련 Q.7과 Q.10 간의 협력으로 OASIS로부터의 표준진행 중인 문서인 SAML 2.0 개정판을 차기 회의(2011년 8월)에서 승인 절차에 들어갈 계획을 갖고 있으며, XACML 3.0 문서는 차년도 2012년 8월에 승인 절차에 들어가는 것을 계획하고 있다.

### 2.3 IPTV

IPTV 정보보호 관련 표준문건은 6개의 표준초안이 개발 중에 있으며, 이번 회의에서는 X.iptvsec-2(X.1192: Functional requirements and mechanisms for secure transcodable scheme of IPTV) 문건이 승인 절차에 들어갔으며, 차기 회의에는 X.iptvsec-3(Key management framework for secure IPTV services),

X.iptvsec-4(Algorithm selection scheme for service and content protection(SCP) descrambling)와 같은 2건의 표준초안에 대하여 승인절차에 들어갈 예정에 있다.

신규 IPTV 정보보호 표준안으로 이번 회의에서는 X.iptvsec-8: Virtual machine-based Security platform for renewable IPTV SCP(Service and Content Protection) 표준 작업 아이템에 대한 채택이 있었다. 내용은 IPTV 서비스 환경에서 SCP 에 대한 서비스 갱신을 위한 가상머신 기반의 정보보호 플랫폼 구성에 관한 아이템이다.

### 2.4 Cybersecurity Index

X.csi(Guidelines for cybersecurity index) 표준초안은 사이버공간에서 정보보호 안전성을 평가하는 지수 개발을 목표로 하며 이번 회의에서는 보안지수를 설정하기 방법론과 지수를 정하는 절차에 대한 기고가 있었으며, 토의를 통하여 본문에 적용할 것을 합의되었다. 기관이나 국가의 사이버공간의 보안지수를 측정하기 위한 지표와 방법을 제시하는 것은 향후 사이버 공간의 안전성을 평가하는 주요 지수가 될 수 있기 때문에 각국 간의 이해가 집중되는 표준초안이 된다. 본 문건에 대하여는 한국의 염흥열 교수가 에디터로 대응하고 있다.

### 2.5 Cloud Security

클라우드 정보보호 관련하여 이번 회의에서 열띤 토의가 있었으며, 주로 어떤 내용을 어떤 Question에서 업무 담당을 하는 것이 적절한 것인가 하는 토의가 이루어졌다. 회의가 진행되면서 점점 다음 회기 구조조정에 대한 포석이 짙어졌으며, 이에 대한 적극적 대응이 국가적으로 필요하다고 사료된다(TD1815). Q.8이 리드 Question이 되고, Q.3, Q.4, Q.7 그리고 Q.10이 협력을 하며, 차기 회의에 Q.8은 클라우드 정보보호에 대한 업무분장에 대한 초안을 제시하는 것으로 결론지었다.

### 2.6 Smart Grid Security

스마트 그리드 관련해서는 RFID 및 센서 정보보호를 검토해온 Q.6에서 관리하는 것으로 진행하며, 지난 1월 FG-smart의 5차 회의 결과로 계획하고 있는 주요 Deliverable로서 스마트그리드 개요, 유스케이스, 요구사항, 구조, 용어를 계획하고 있음을 알려왔고, SG17에서는 향후 업무 협력을 위한 응답 업무연락을 보내는 것으로 대응했다(TD1487).

### 2.7 Child Online Protecton

지난 2월에 있었던 TSAG 회의에서는 COP(Child Online Protection)의 연구 토픽을 SG17이 수행할 것을 결의했으며, 또한 콘텐츠의 내용을 검색하지 않는 환경에서 COP에 대한 적절한 토픽을 조사할 것을 코멘트 하였다. 이에 후속 작업으로 SG17에서는 특별 이슈로 토론이 있었으며, CG on COP를 결성하였고 TOR(Terms of Reference, TD1766 Rev.1)을 작성했으며, 컨비너로 한국의 나재훈을 임명하였다(TD1840). ToR의 주요 내용은 다음과 같다.

- CG는 COP관련 활동이나, 이니셔티브가 있는지에 대한 조사와 기술적 배경에 대한 조사하여 SG17에 그 결과를 보고한다.
- CG는 다음 SG17 8월 회의 21일 이전에 보고한다.
- CG는 SG17 내의 기술적 측면과 자원의 효율적 이용과 중복업무에 대하여 고려한다.

## 3. 맺음말

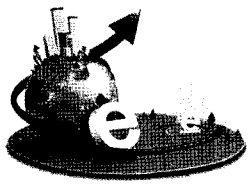
ITU-T SG17회의에서 한국, 일본, 중국은 표준 기고서 제안이 왕성한 국가들이다. 수년 동안의 투자와 노력에 의하여 SG17에서의 한중일의 역할은 매우 중요한 위치에 이르렀고, 또한 한중일의 협력도 상당히 좋은 분위기에 올라와 있다. 이러한 측면에서 SG17의 차년도 의장이 누가 될 것인가는 중요한 사안이 될 수 있다. 그

렇지만 현재의 의장(Mr. Kremer, 러시아)이 연임을 목표로 하고 있다는 의지가 엿보이고 있는 가운데, SG17 구조조정을 재미있는 양상을 보일 것이라고 생각된다. 또한 한국은 이러한 구도하에서 좋은 입지의 위치를 선점 할 수 있는 좋은 재료들이 있는 가운데 관망하는 자세가 필요하다고 사료된다.

정보통신 용어해설

## 스팸 릴레이

**Spam Relay [정보보호]**



보안이 취약한 메일 서버의 릴레이 기능을 이용하여 스팸메일을 보내는 것.
메일 서버를 정당한 권한 없이 스팸메일 서버로 악용하는 것이다. 스팸 릴레이 공격이 진행되면 대량의 이메일을 송・수신하기 위해 네트워크 트래픽이 증가해 정상적인 이메일 수신을 방해할 수도 있다.